
تجارب شخصية مع الفيروسات
مشاكلها و حلولها
(الجزء الأول)
bitdefender
ESET
AVIR
M
لكاتبه
فهد سعيد مقرم

أعوذ بالله السميع العليم من الشيطان الرجيم

وما أوتيتم من العلم إلا قليلا

صدق الله العظيم



إهداء

إلى الغاليين والدايّ وإخوتي
إلى جميع المسلمين في كل مكان و زمان
إلى كل طالب معرفة في هذا المجال الحاسوبي الواسع
أهدي هذا الجهد المتواضع



الفهرس

الموضوع	رقم الصفحة
نبذة عن كاتب الموضوع	5
المقدمة	
أسباب الإصابة	7
صور للفيروسات	8
كيف يتم تفعيل الفيروس؟	11
المشاكل التي تحدثها الفيروسات؟	11
كيف أعرف إن الجهاز مصاب؟	12
التجارب الشخصية	
OSO.exe	14
New Folder.exe	15
NIDEIECT.com	15
Sservice.exe	17
Pagefile.pif	17
zPharaoh.exe	18
Ctfmon.exe	19
طرق الوقاية والعلاج	
طرق الوقاية	21
العلاج	24
أسئلة وإضافات الأعضاء	
أسئلة و إضافات الأعضاء بموضوعي بالمنتدى	27
خاتمة	
ما هو واجبك تجاه الموضوع	32
طلب صغير	32
نصيحة بعنوان (لا تنسَ)	33



نبذة عن كاتب الموضوع

الاســــــــــــم : فهد سعيد حيمد مقرم
تاريـــخ المـــيلاد : 27- 07- 1983
الديانــــــــــــة : مسلم لله الحمد و المنة
الجنسيـــــــــــة : يمني من منطقة حضرموت شبام - قرية الحزم و أعيش بالسعودية - جدة
الدرجة العلميــــة : بكالريوس في علوم الحاسوب من جامعة حضرموت للعلوم و التكنولوجيا
الهوايـــــــــات : كل ما يتعلق بالحاسوب من برامج و حماية و تصميم و غيره
الحالة الاجتماعية : عازب ربنا ييسر بنت الحلال
الوظيفـــــــــة : بالانتظار أسأل الله الرزق الحلال
اسمي بالمنتـــدى : MaskFD
البريد الالكترونــي : Maskfd77@hotmail.com



المقدمة



بسم الله الرحمن الرحيم

الحمد لله . . والصلاة والسلام على خير خلق الله . . وعلى آله وصحبه ومن تبع هداه

قبل البداية في الموضوع

هذا الموضوع كتبته بمنتدى المشاغب بتاريخ (29-11-2008) و قمت هنا بتحويله لكتاب بصيغة PDF بتاريخ (09-08-2009) للنشر و التوزيع للفائدة العامة .. و أعتذر منكم على القصور في ترتيبه و تنسيقه لضيق وقتي .. أرجو لكم الفائدة و المتعة ..

بعض الملاحظات قبل بداية الشرح أرجو قراءتها

1- هذا الموضوع كتب لمعرفة طرق الوقاية والعلاج من الإصابة بالفيروسات .. لذلك لا يسمح باستخدامه للإضرار بأجهزة الآخرين.
2- المعلومات المذكورة بالدرس هي مجرد اجتهاداتي الشخصية .. يعني تقبل الخطأ والصواب و المناقشة .. لذلك أنا غير مسؤول عن أي أضرار تنتج عنها (رغم عدم وجود الأضرار لكن للاحتياط).

المقدمة

لا يكاد أحد يسلم هذه الأيام من الفيروسات .. صارت زي التحلية مع الكمبيوتر .. يكتشفوا واحد يطلع ألف .. وكل فترة يتفرمت الجهاز وتعيد تحميل البرامج وتفقد بيانات هامة بسببها .. في هذا الدرس كتبت تجاربي الشخصية معاها وبعض من أسباب الإصابة وطرق الوقاية والعلاج اللي أعرفها.

أسباب الإصابة

معظمها يجي من الإيميل أو الفلاش ميموري Flash Disk و البرامج والكراكات غير موثوقة .. لكنها غالباً لا يتم تفعيلها إلا إذا نقرت عليها نقراً مزدوجاً لأنها برامج تنفيذية .. فيه أنواع تعمل بدون نقر أعتقد يسموها برامج سكربت Script Programs لا أعرف عنها الكثير وأعتقد إلغاء خاصية Script من الجهاز يمنع عملها لكنها ليست موضوعي ..
أول شيء هذه بعض الأمثلة لأشكال الفيروسات:

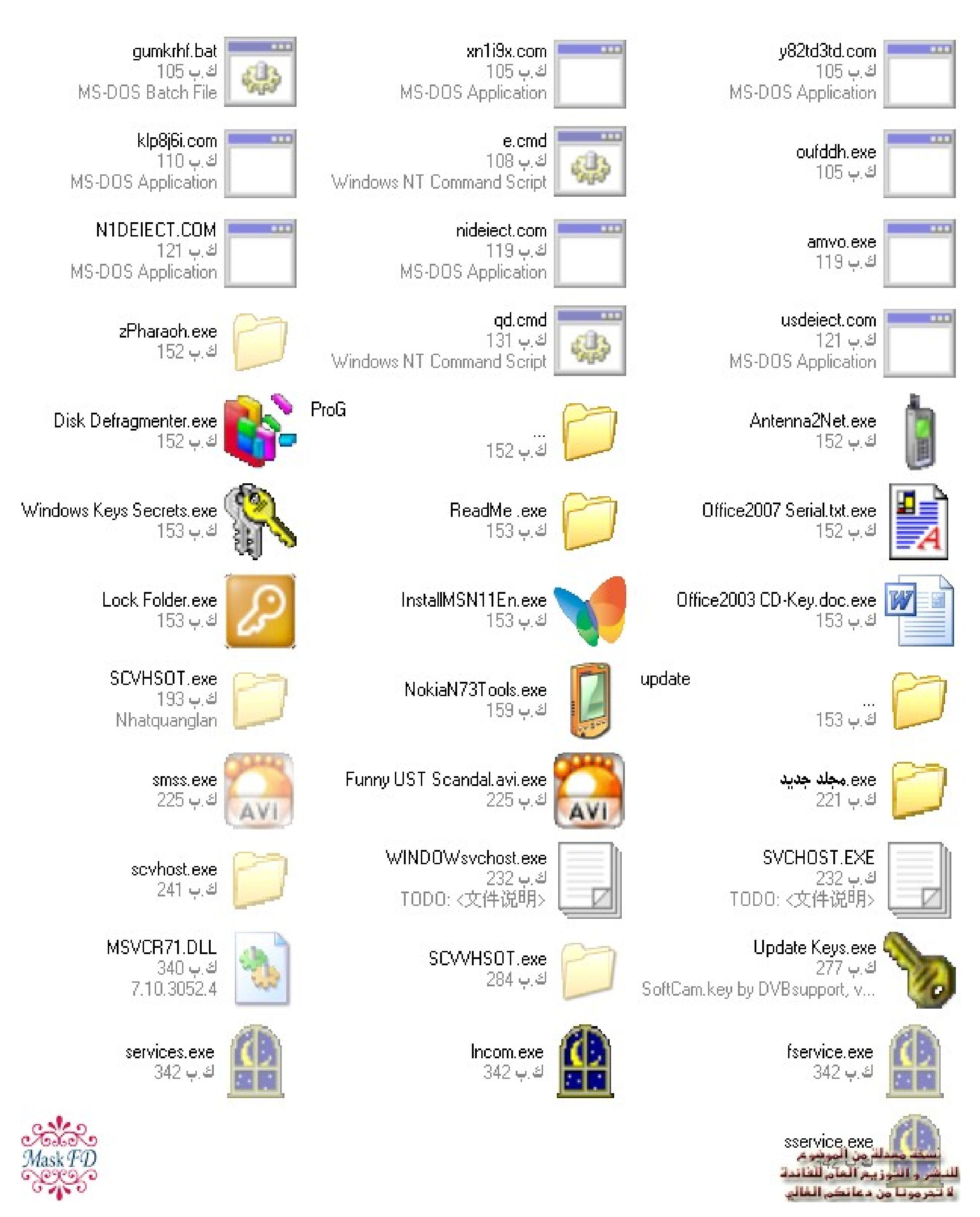


صور للفيروسات

Recycled	AUTOEXEC.BAT 1 ك ب MS-DOS Batch File	autorun.inf 1 ك ب معلومات الإعداد هذا ملف يرافق الفيروس لتشغيله وليس فيروس
copy.exe 2 ك ب	pagefile.exe 8 ك ب	auto.exe 14 ك ب
autoupdatev2.exe 20 ك ب	MDM.EXE 22 ك ب	winkey.dll 24 ك ب 1.0.0.1
WMPLAYER.EXE 24 ك ب Windows Media Player	Windows.scr 28 ك ب Screen Saver	REDIR32.EXE 32 ك ب Win32 REDIR32 core compon...
SETUP.EXE 35 ك ب	reginv.dll 36 ك ب	REGWIZ.EXE 36 ك ب RegWizExe
SKY.EXE 36 ك ب Smart Card Resource Manage...	Sys.exe 36 ك ب	REGSVR32.EXE 37 ك ب Microsoft(C) Register Server
tfidma.dll 38 ك ب	je.exe 40 ك ب	SERVER.EXE 40 ك ب
amvo0.dll 44 ك ب	New Folder.exe 45 ك ب	
INTERNAT.EXE 48 ك ب Internat	RavMon.exe 49 ك ب	secret.exe 51 ك ب
gendel32.exe 52 ك ب	REGENV32.EXE 60 ك ب	host.exe 69 ك ب BindFile Microsoft 基础类应用...
[illegible]	Data MCT.exe 80 ك ب	037589.LOG 93 ك ب مستند نصي



OSO.EXE 95 ك.ب	PAGEFILE 93 ك.ب Shortcut to MS-DOS Program	lsass.exe.38014.exe 93 ك.ب
ntde1ect.com 96 ك.ب MS-DOS Application	tfidma.exe 95 ك.ب	severe.exe 95 ك.ب
un9.cmd 99 ك.ب Windows NT Command Script	tknn6.bat 99 ك.ب MS-DOS Batch File	xp19.com 98 ك.ب MS-DOS Application
H1DWG20.EXE 100 ك.ب	yo2mq6.exe 99 ك.ب	v.cmd 99 ك.ب Windows NT Command Script
b.com 102 ك.ب MS-DOS Application	2ifetri.cmd 101 ك.ب Windows NT Command Script	yew.bat 100 ك.ب MS-DOS Batch File
ylr.exe 102 ك.ب	188qsm.bat 102 ك.ب MS-DOS Batch File	rthrw.com 102 ك.ب MS-DOS Application
t.com 102 ك.ب MS-DOS Application	gjn2pjlw.exe 102 ك.ب	xo8wr9.exe 102 ك.ب
xfoolavp.com 103 ك.ب MS-DOS Application	vy.cmd 102 ك.ب Windows NT Command Script	awda2.exe 102 ك.ب
d.cmd 103 ك.ب Windows NT Command Script	semo2x.exe 103 ك.ب	i.cmd 103 ك.ب Windows NT Command Script
ekugb3.bat 103 ك.ب MS-DOS Batch File	dosocom.com 103 ك.ب MS-DOS Application	juok3st.bat 103 ك.ب MS-DOS Batch File
xpbkh.com 104 ك.ب MS-DOS Application	U.BAT 104 ك.ب MS-DOS Batch File	80avp08.com MS-DO



لاحظوا إن امتداد الفيروس غالباً يكون **exe,cmd,scr,com,bat** أما الامتدادان **log & dll** فالفيروس بداخلهم ولا ينفذ مباشرة .

حجم الفيروس غالباً صغير بالكيلو بايت.

معظمها مخفية ولا يمكن جعلها مظهرة لأن خاصية الإخفاء ملغية كما بالصورة:





إذا كانت ظاهرة تكون بأشكال متعددة مثل شكل المجلد أو المفكرة أو برنامج عشان تغلط وتنقر عليها ويشتغل الفيروس (توجد أمثلة كثيرة لأشكالها المتعددة في شرح فيروس zPharaoh).

السؤال هنا كيف يتم تفعيل الفيروس؟

عادة مع الفيروس يجي ملف أوتورن - بمعنى تشغيل تلقائي - autorun.inf ينسخ على سطح الفلاش ميموري Flash Disk أو الهاردسك Hard Disk .. هذا الملف يستخدم في السيديات CD Autorun لتشغيل تطبيق معين له واجهات أو عرض ما .. لكنه يوضع مع الفيروس لكي يتم تشغيله بواسطته.

المشاكل التي تحدثها الفيروسات؟

إخفاء المجلدات والملفات المخفية ومنع الوصول لخيارات المجلد Folder options وإدارة المهام Task Manager ومحرر تسجيل ويندوز Windows Registry واستهلاك موارد الجهاز الذي يؤدي إلى بطء الجهاز الملحوظ.
تكمن الخطورة إذا كان الفيروس من النوع الذي ينتشر في الجهاز ويصيب كل برنامج وتطبيق وصفحات الانترنت وملفات النظام.



كيف أعرف إن الجهاز مصاب؟

غالباً الفيروس ينسخ نفسه وملف الاوتورن على كل الأقراص الصلبة .. لكن إذا أصابك لن تستطيع الوصول لخيارات المجلد لإظهار الملفات المخفية و أيضاً إظهار ملفات النظام لأن الفيروس يعتبر كملف نظام و لا أدري كيف يتم تحويله بهذه الطريقة .. عشان كذا لازم يكون عندك برنامج الضغط الوينرار WIN RAR ممكن تستغرب أيش دخله بالموضوع؟!

هذا البرنامج يظهر جميع الملفات المخفية دائماً من داخله و لا يتأثر غالباً بالفيروسات .. يعني تروح للقرص الصلب من داخل البرنامج وتشوف إذا حصلت ملف autorun.inf ومعه تطبيق غريب أول شيء تفتح autorun.inf لا يضر فتحه لأنه زي المفكرة .. إذا كان بداخله اسم التطبيق معناه إنه فيروس مثل الصيغة التالية:



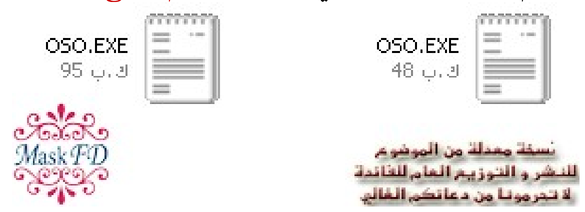


التجارب الشخصية مع الفيروسات

هنا أشرح بعض الفيروسات التي أصابت جهازي أو أجهزة زملائي والملاحظات عليها:

OSO.exe

هذا الفيروس جاء على شكل مفكرة بحجم 95 KB ومرة أخرى بحجم 48 KB .. مع هذا الحجم البسيط اعتقدت إنه فعلاً ملف مفكرة لكن لما فتحته لم يفتح شيء وهنا عرفت إنه فيروس خاصة بعد ظهور اسم تطبيق غريب في إدارة المهام Task Manager .



ينسخ هذا الفيروس نفسه بأسماء مختلفة لها نفس الحجم هي:
severe.exe و tfidma.exe و tfidma.dll .. ملف النظام الأخير حجمه 38 KB في مجلد النظام System بالنسبة لنظام Windows ME و مجلد System32 بالنسبة لنظام Windows XP .. النوع الثاني اللي حجمه 48 KB ضرره أقل ولا ينسخ نفسه في مجلد النظام.



ثم يعمل مع بدأ التشغيل عشان ما تقدر تحذفه بشكل مباشر لو قدرت تشوفه.



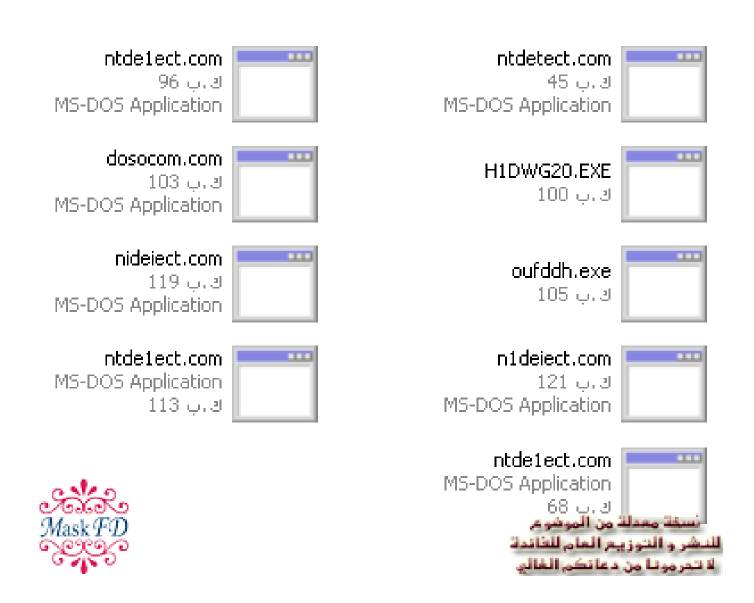
New Folder.exe

هذا فيروس قديم معروف أيضاً باسم مجلد جديد بس للي ما يعرفه .. طريقة عمله هي إنه يعمل داخل كل مجلد نسخه منه لها نفس اسم المجلد وكلها بحجم الفيروس الأصلي .. لاحظوا أن الامتداد تنفيذي EXE لكن هذا الامتداد لا يظهر إلا إذا أظهرنا امتداد الملفات من خيارات المجلد.



NIDEIECT.com

وهذا الفيروس له أنواع كثيرة يتغير فيها الاسم قليلاً وأنواع أخرى مختلفة في الاسم لكن جميعها لها نفس العمل كما في الصورة.



هذا الفيروس مشابه لـ OSO.exe في ناحية انك ما تقدر تحذفه مباشرة لأنه يرجع مرة ثانية في جميع الأقراص لأنه ينسخ amvo.exe و amvo0.dll إلى مجلد النظام System32 وثم يضعهم في قائمة بدء التشغيل.

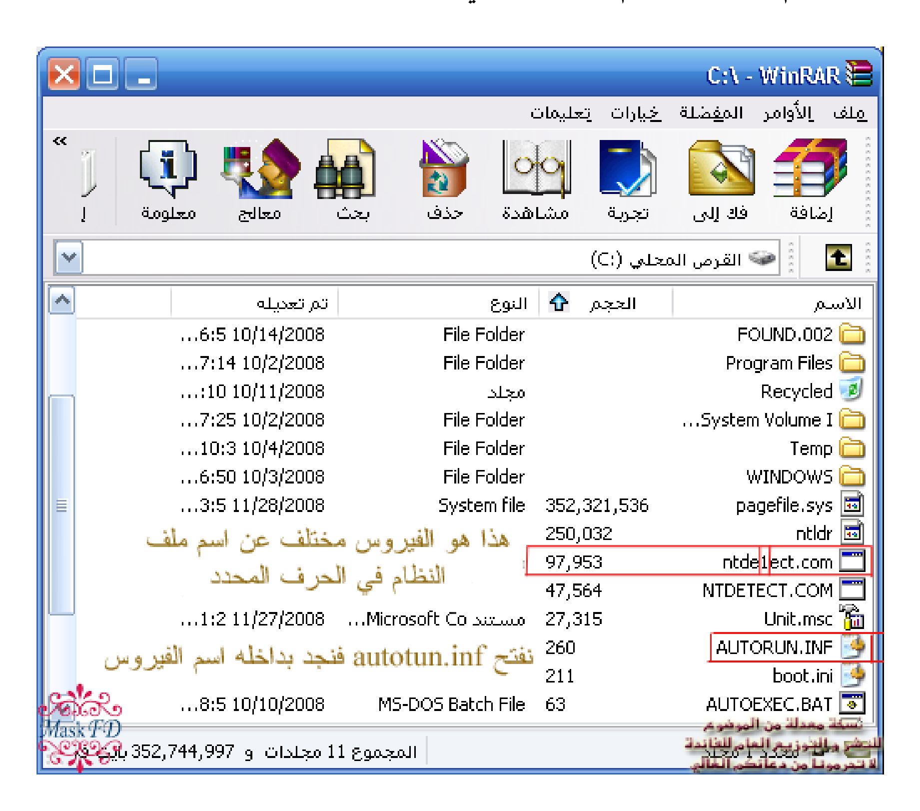








اسم هذا الفيروس يشبه اسم **ملف النظام** الموجود على قرص C وهو **NTDETECT.COM** لذلك أرجو الحذر من الخلط بينهما .. عندي زميل اعتقد إنه فيروس فحذفه فاضطر يفرمت الجهاز لذلك لازم تتأكد من اسم الفيروس في ملف **autorun.inf** عشان تحذفه.







الفيروسات أحياناً تأخذ أسماء ملفات نظام مثل **NTDETECT** و **CTFMON** و **SMSS** و **SCVHOST** و **CSRSS** لذلك يجب الحذر عند حذفها .. والأفضل تغيير امتداد الملف المشكوك فيه إلى امتداد غير تنفيذي عشان في حالة حصلت مشكلة بسببه تقدر ترجع الملف عن طريق نظام تشغيل يقلع من السيدي مباشرة مثل **Windows Pre-installation Environment**.

Sservice.exe

ينسخ نفسه في مجلد النظام **System** بثلاث أسماء هي **fservice.exe** و **services.exe** و **Incom.exe** لكن الحجم وشكل الأيقونة هو المشترك بينهم .. عمل بطء وأضاف قيم في الملف win.ini تخليه يعمل بنسخ كثيرة في الذاكرة هذا في نظام **Windows ME** .



Pagefile.pif

هذا الفيروس الصيني المعروف اللي سوى بلاوي للناس قبل فترة .. يمكن 8 أشهر .. أصاب الجهاز عندي بسبب غلطة .. دخلت القرص بالنقر بالزر الأيمن ثم الأمر فتح وهذا شغل الفيروس .. وتسبب بحذف أكثر من 8500 برنامج وصفحة انترنت من جهازي خلال يومين فقط من إصابته للجهاز. يشبه ملف الدوس في الأيقونة ولا يخفي عرض الملفات المخفية عندما يتم تفعيله .. لذلك لم أكتشفه بسرعة .. **فقط يخفي إظهار ملفات النظام** و بعدها يبدأ من قرص C إلى آخر قرص بنسخ نفسه في كل برنامج و صفحة انترنت .. وأكيد إذا استخدمت برنامج فيروسات بعدها بيحذف ملفات نظام التشغيل وبيكون لازم تفرمت الجهاز .. لكن بالأساس لايمكنك الفيروس من تحميل البرامج ويمنع فتح بعضها .. مثل **WinRAR** و **Realplayer**.







zPharaoh.exe

هذا الفيروس مشابه في كبر أضراره لفيروس Pagefile أيضاً ظهر قريب .. تقريباً نفس الوقت لكنه تميز بأنه ينسخ نفسه في كل مجلد في الجهاز بأسماء و أيقونات و أحجام مختلفة .. هذا بالإضافة لنسخه نفسه في معظم البرامج .. وأكيد الجهاز لازم يتفرمت بعدها.

للمعلومة أنا لم أصاب بهذا الفيروس لكنني أدخلت الهاردسك الخارجي Hard Disk في جهاز مصاب مدة تقارب الربع ساعة وكان قد نسخ نفسه بأكثر من 600 برنامج .. في الصورة بعض الأشكال المختلفة التي ينتجها هذا الفيروس.





Ctfmon.exe

يخفي نفسه هذا الفيروس داخل مجلد بأيقونة سلة المحذوفات **Recycled** لكن ملف **autorun.inf** يفضح موقعه كما بالصورة.







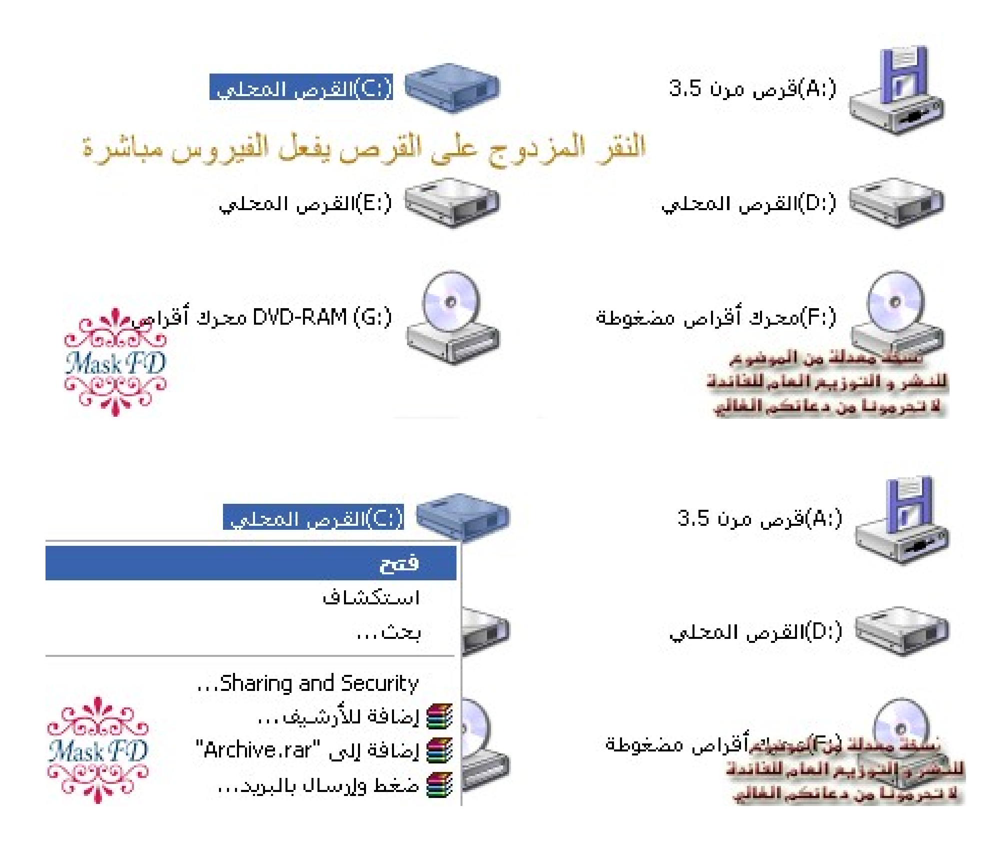


طرق الوقاية والعلاج



طرق الوقاية

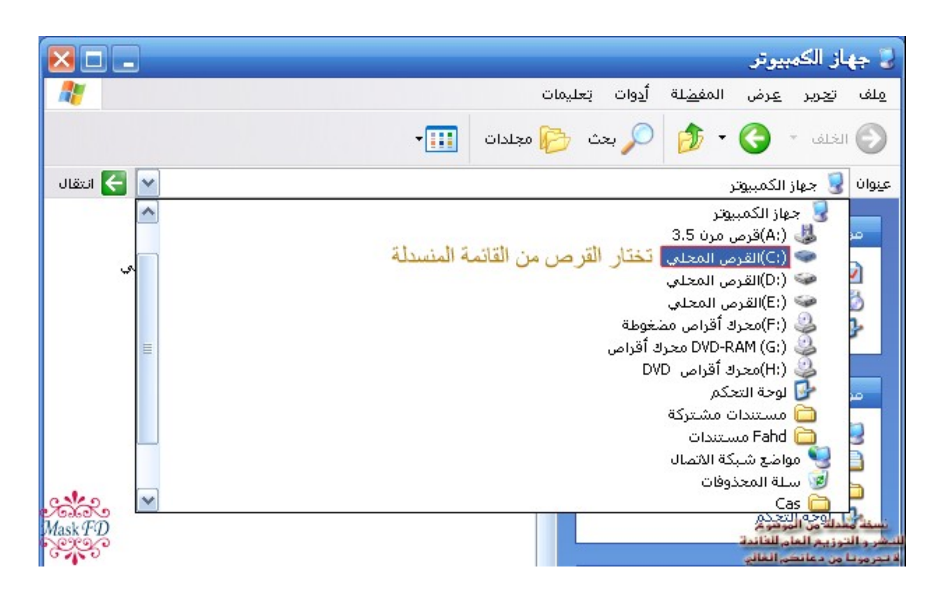
أولاً حدث برنامج الفيروسات أولاً بأول لتقليل احتمال الإصابة بالفيروسات لا يهم ماهو نوع البرنامج إذا لم يتم تحديثه دورياً.
ثانياً لا تعتمد اعتماداً كاملاً على برنامج الفيروسات .. لأنه إلى أن تكتشف شركة البرنامج المضاد للفيروسات الفيروس الجديد يكون هذا الفيروس أصاب الآلاف .. وقد تكون لا قدر الله منهم ..
عشان كذا انتبه من البرامج والكراكات الغير مضمونة ولا تتهاون فيها .. الملفات التي ترسل في المحادثات أو الجروبات على أساس إنها صورة أو فيديو ممكن تكون مدمج معها فيروسات .. وأهم نقطة لا تفتح الفلاش ميموري Flash Disk بالنقر المزدوج أو بالنقر باليمين ثم الأمر فتح ..
هذه الطريقتين تشغل الفيروس



الطريقة الآمنة والمجربة عند كثير من زملائي هي الدخول من مستكشف ويندوز (Windows Explorer) .. إما من أيقونة مجلدات (Folders) التي في أعلى الصفحة حق جهاز الكمبيوتر أو من قائمة إبدأ (Start).. ثم البرامج (Programs) .. ثم البرامج الملحقة (Programs accessories) .. ثم مستكشف Windows (Windows Explorer) .



أو من **الشريط** الموجود أعلى الصفحة المحتوي على الأقراص الصلبة.



ثالثاً عند توصيل الفلاش ميموري Flash Disk لازم تستمر بالضغط على مفتاح Shift إلى أن ينتهي التعرف على الفلاش .. هذه الطريقة مهمة جداً في نظام Windows ME أما في نظام Windows XP فمن باب الاحتياط .. لأنه قد يدخل مباشرة للفلاش بدون إظهار النافذة التالية و لاحظوا في الصورة أن الفيروس هو التطبيق الأول غير المعروف .




(Q:) Jonamo
يحتوي هذا القرص أو الجهاز على أكثر من نوع واحد من المحتوى.
ماذا تريد أن يفعل Windows ؟
تشغيل البرنامج
استخدام البرنامج الموفر على الجهاز
Create jetAudio's album
استخدام jetAudio
Play
استخدام jetAudio
Play Music
استخدام Media Player Classic
Play Media Files
استخدام RealPlayer
تشغيل
موافق
إلغاء الأمر
نسخة معدلة من الموضوع
للنشر و التوزيع العام للفائدة
لا تحرمونا من دعائكم الغالي



العلاج

الفيروسات اللي تنتشر زي الدودة مثل **zPharaoh.exe** و **Pagefile.pif** مالها علاج غالباً غير إنك تفحص الجهاز أولاً ببرنامج فيروسات محدث .. بعد الفحص النظام ما راح يقلع لأنه ملفات النظام أيضاً أصيبت بالفيروس .. وثانياً تحمل النظام من أول وجديد أو تعمل **تهيئة (فورمات Format)** من البداية .. وأهم نقطة تحذف كل البرامج اللي كانت على الجهاز ذلك الوقت أو تفحصها بعناية شديدة عشان ما يرجع لك الفيروس أو ينتقل لغيرك.

أما الفيروسات العادية التي تنسخ نفسها على الأقراص الصلبة فقط فيمكن حذفها من كل الأقرص وتنتهي مشكلتها .. يمكن حذفها ببرنامج مثل **anti_autorun** أو مباشرة ببرنامج **win rar** تحذفها من كل قرص ..

هناك فيروسات تنسخ نفسها على الأقراص الصلبة وأيضاً داخل مجلد **System32** عشان ما تقدر تحذفها لأنها تعيد نسخ نفسها كلما حذفتها .. وعلاجها أولاً إنك تعرف اسم البرنامج المنسوخ داخل مجلد النظام **System32** مثل ما ذكرت في فيروس **OSO.exe** كان ينسخ **severe.exe** و **tfidma.exe** و **tfidma.dll** وكان يضع التطبيقين في قائمة بدء التشغيل و مثل **NIDEIECT.com** وهو منتشر كثيراً والذي ينسخ **amvo.exe** و **amvo0.dll** إلى مجلد النظام **System32** ويضع التطبيق **amvo.exe** في قائمة بدء التشغيل .. وحذف هذا النوع بدون برنامج مضاد فيروسات يكون كالتالي:

أولاً تلغي الفيروس من بدء التشغيل .. تفتح **قائمة أبدأ Start Menu** ثم الأمر **تشغيل Run** ثم تكتب الأمر **msconfig** يظهر لك نافذة تختار **التبويب بدء التشغيل Start up** وتشيل علامة الصح من الفيروس .. راجع مثال **NIDEIECT.com** و **amvo.exe** بالأعلى ...





☑	RunDll32 cwcprops	RunDll32 cwcprops.cpl,CrystalControlWnd
☑	realsched	\Program Files\Common Files\Real\Update_OB"
☐	amvo	C:\WINDOWS\system32\amvo.exe
☑	Utility Tray	C:\WINDOWS\system32\sistray.exe
☐	avgnt	\Program Files\Avira\AntiVir PersonalEdition Cla"
☐	msmsgs	Program Files\Messenger\msmsgs.exe" /backg"

ثانياً تعيد تشغيل الجهاز ثم تحذف الفيروس من جميع الأقراص الصلبة و تحذف amvo.exe و amvo0.dll من C:\WINDOWS\system32 لكن الفيروس مخفي لذلك لازم تحذفها كلها عن طريق استخدام برنامج win rar واستخدام أداة البحث التابعة للبرنامج لإيجاد الفيروس.

تبقى بعض آثار الفيروس مثل عدم ظهور الملفات المخفية وإدارة المهام وغيرها ..
يمكنك إرجاعها ببرنامج مثل RRT Remove Restrictions Tool .. لايوجد لدي رابط لكنه موجود بالمنتدى.
(تمت إضافته و روابط أخرى بالجزء الثاني)

تم بحمد الله و شكره و توفيقه.



أسئلة وإضافات الأعضاء

أسئلة و إضافات كانت بموضوعي بالمنتدى أحببت إضافتها للفائدة.
تم اختصارها لأخذ الفائدة منها فقط مع جزيل الشكر لكل من سأل و أضاف للموضوع.

مشاركة للأخ الكريم Amer Asran

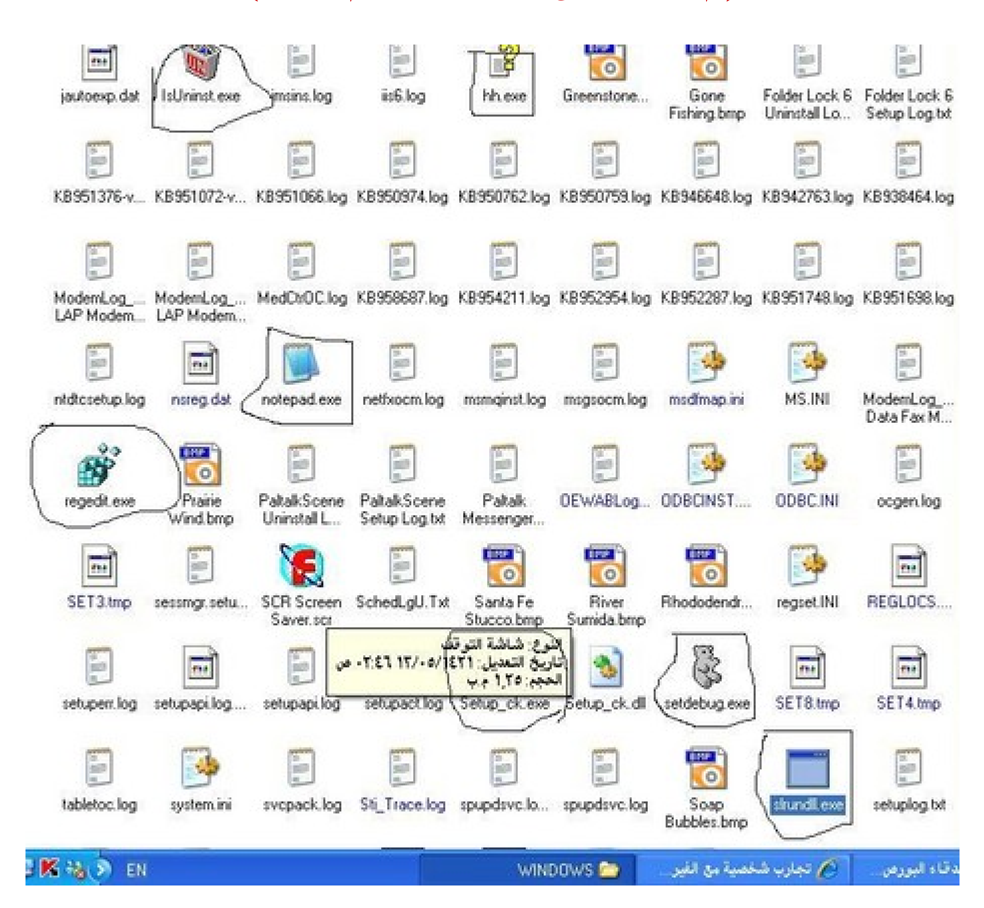
تعليق بسيط وتصحيح لاحد المعلومات Ctfmon.exe هذا ليس فيروس ولكنه تطبيق اساسي في اي نسخه ويندوز ووظيفته التحويل بين اللغات عن طريق الكيبورد.

الرد :

أنا ذكرت إنه Ctfmon من ملفات النظام في شرحي لفيروس NIDEIECT.com وأشكرك لأني لم أكن أعرف وظيفته .. وطبعاً ملف النظام Ctfmon بيكون موجود بمجلد النظام System32 لكن هذا الفيروس وجدته في CD و اكتشفه الكاسبر سكاي و الأفيرا .

مشاركة للأخت الكريمة تيماء

الامتداد exe كثير بجهازي هل كلها فايروسات ؟؟؟؟ وكيف اتعامل معها؟
(تم التعديل على الصور لكبر حجم أبعادها)





الرد :

الامتداد exe يعبر عن تطبيق يعمل بعد النقر عليه .. والمعنى إن الفيروس تطبيق مثله مثل أي برنامج آخر .. لكن الفرق في أهداف التطبيق .. الفيروس هدفه التخريب أو التجسس أما البرامج الأخرى تجارية أو تعليمية .. إلخ .. يعني ليس كل ملف امتداده exe فيروس ولكن الفيروس ممكن يجي بهذا الامتداد .. مثل الامتداد scr هذا مخصص لشاشة التوقف لكن بعض الفيروسات تتنكر بصيغته ..الملفات التي أشرتي إليها موجودة بمجلد النظام Windows هذه ملفات نظام التشغيل ويندوز لا يمكننا حذفها أو التعديل عليها والا بيخرب النظام .. مثل notepad.exe هذا برنامج المفكرة .. و regedit.exe هذا محرر التسجيل لويندوز المعروف بالريجيستري..

متى نشك بأن ملف معين فيروس؟

إذا كان الملف موجود على سطح جميع الأقراص الصلبة C,D,E, ومعه ملف autorun.inf إذا كان الفيروس فعلاً بالجهاز ما راح نتمكن من رؤيته لذلك نفتح برنامج الضغط winrar لأنه يعرض جميع الملفات حتى لو كانت مخفية .. ثم ندخل على جميع الأقراص إذا وجدنا ملف autorun.inf نفتحه .. بيظهر لنا اسم الفيروس بداخله اللي غالباً يكون امتداده exe,scr,com,bat,cmd وقتها ممكن نحذف الفيروس وإذا ما انحذف ممكن تراجعي الشرح في أول صفحة .. آخر جزء بالشرح ..

المشكلة إن الفيروس ممكن يدمج نفسه بداخل برنامج عادي .. هنا لا يمكن كشفه إلا ببرنامج مضاد للفيروسات .

مشاركة للأخ الكريم almhajar

بالنسبة لفيروس zPharaoh.exe فهذا فيروس خطير ظننت أن ملفاتي كلها راح تندمر .. لكن بعد فحصه بالكاسبر الثامن .. قام بتطهير كل الملفات المصابة دون المساس بها او الضرر بها .. حتى رجعت ملفاتي كلها سليمة

الاستفادة :

ليست جميع برامج الفيروسات تحذف البرامج الملوثة بالفيروسات .. يعني لو عندك برامج هامة حاول تعمل منها نسخ و نوع فحصها ببرامج الفيروسات .. يمكن أحدها يقدر ينظفها بدون الحذف الكامل .

مشاركة للأخ الكريم المسار

انا مرت على اغلب هذه الفيروسات والشرح موفق 100/100 لكن السؤال كيف يتم تفعيل الاوتورن عند صنع الفيروس وانتشاره على الاجهزة ؟
بمعنى
لما تصنع الفايروس يكون بدون اوتورن كيف يتم تفعيل الاوتورن ؟

الرد :

أعتقد حسب التجربة إنه الفيروس بينشئ ملف الأوتورن بنفسه كل ما تم تفعيله أو النقر المزدوج عليه يعني ملف الاوتورن مجرد وسيلة لفتح الفيروس .

مشاركة للأخ الكريم mostafaseb

لدى معلومة اود اضافتها اغلب المناطق فى الجهاز المصابة بالفيروسات تكون فى مجلدات ذكرت انت منها واحدة و هو Recycled و الثانى و ارجو الانتباه اليه و هو ما بداخل مجلد System Volume Information و هذا الملف يكون مخفيا و لاظهاره نتبع الاتي :
بداخل جهاز الكمبيوتر My computer توجد قائمة علوية
نختار منها أدوات tools ثم خيارات المجلد Folder Options ثم عرض View
سنجد الملفات و المجلدات المخفية hidden files and folders
ضع علامة على أظهر الملفات المخفية و المجلدات Show hidden files and folders
و اسفلها بقليل ستجد
اخف ملفات نظام التشغيل المخفية (مستحسن)
(Hide protected operating system files(recommended
ازل العلامة من عليها سيظهر لك مربع تحذير اضغط ok
ثم ok
الأن ادخل لل C و ستجد الملف حاول ان تحذف ما به و هكذا ستجده فى بقية الاقراص
ثالثا/ لأحظت مجلد بعنوان pchealth فى هذا الامتداد C:\WINDOWS\pchealth
به فيروسات لا يكتشفها و يزيل الفيرس سوى برنامج طرح من قبل فى المنتدى Smart cop
ارجو التحقق من كلامى على انظمة XP .

الرد :

أشكرك على إضافتك الرائعة للموضوع ..
فعلاً الفيروسات تنسخ نفسها في مجلد النظام System Volume Information
لكنها ما كانت تتفعل من هذا المكان .. احتمال تتفعل مع استعادة النظام System Restore
بالنسبة لـ pchealth ما كنت أدري إن الفيروسات تنسخ فيه لازم آخذ حذري من هذا المجلد أيضاً .

مشاركة للأخت الكريمة نورعبدالمعز

يعني ايه برنامج win rar اللي اعرفه انه برنامج ضغط يا ريت تشرح ازاي بيشيل الفيروسات وخاصة فيروس new folder.

الرد :

فعلاً برنامج win rar حق ضغط الملفات لكن فيه ميزة وهي انه يعمل مثل المستكشف .. يظهر الملفات المخفية و ملفات النظام حتى لو كان عندك فيروس يمنع ظهورها .. هذا يفيد لو كان الفيروس مثلاً مثل new folder أيقونته شكلها مجلد و هذا اللي يخدعنا فيه ..لما تفتح win rar و تشوف هذا الفيروس أولاً بتظهر أيقونته أيقونة تطبيق و ليس مجلد .. ثانياً بيظهر امتداده exe و المجلد طبعاً بدون امتداد .. يعني إذا شكيت في ملف و تأكدت من امتداده exe,com,bat,scr فهذا بيعطي احتمال كونه فيروس خاصة لو كان اسمه و شكل ايقونته مشبوهان ..
فيروس مثل new folder بيكرر نفسه في كل مجلد بنفس اسم المجلد .. يعني لو عملنا بحث و يفضل البحث من داخل win rar لجميع الملفات بنلاحظ إن ملفات كثيرة بتظهر بنفس الحجم و أسماء مختلفة .. حجم الفيروس بالكيلو بايت موضح في الصفحة الأولى للشرح ..

مشاركة للأخ الكريم محمد المريش

عند الفحص بالكاسبر سكاي أجد هناك بعض ملفات البرامج لايستطيع النفاذ اليها (لاتُفتح له) فهل هذا طبيعي أو انها تحتوي على فيروسات .

الرد :

برامج الفيروسات عموماً لا تستطيع الدخول على الملفات المشفرة مثل الملفات المضغوطة المحمية بكلمة سر .. وهذه الطريقة هي اللي أحفظ بها الفيروسات على الجهاز عشان ما يكتشفها برنامج الحماية .. يعني ممكن البرامج اللي ما يقدر الكاسبر يدخلها مشفرة .. والله أعلم .



خاتمـــة



خاتمة الموضوع

هذا الجهد المتواضع و المليء بالقصور إهداء لكل المسلمين .. أتمنى يفيدكم و يعينكم بعد الله على التخلص من الفيروسات و فهم آليات عملها .

ما هو واجبك تجاه الموضوع

الموضوع كتب للفائدة العامة .. و كنت أتمنى نشره و توزيعه بصورة كبيرة .. لكني لأسف لم أتمكن من ذلك ..
لذلك واجبك أخي الكريم أختي الكريمة أن توزعوه لمن يحتاجه .. لأنه من نشر العلم و كتمه إثم و مضرة عامة .. حيث أن هدف الموضوع هو حماية أجهزتنا من الفيروسات .

و طلب صغير

وهو عند الله كبير .. دعاء بظهر الغيب لكاتب الموضوع .. يعلم الله كم أخذ هذا الموضوع من وقتي و كم بذلت في ترتيبه و تنسيقه و تصميمه لإيصاله لكم بهذه الصورة المتواضعة ..
فلا تحرموني من دعائكم الطيب بظهر الغيب و والدي و أهلي و أقاربي و المسلمين بالمغفرة و الهداية و الرحمة و الرزق الحلال المبارك و دعاء خاص لوالدتي بالشفاء العاجل .. و أسأل الله العظيم الكريم لكم أضعاف ذلك .

للتواصل

لمن يريد التواصل معي يمكنه مراسلتي على هذا الايميل .. لكني لا أعدكم بشيء لأني مشغول جداً هذه الفترة من حياتي ..
Maskfd77@hotmail.com

بارك الله فيكم و وفقكم لما يحبه و يرضاه .



نصيحة بعنوان (لا تنسَ)

نصيحة بعنوان لا تنسَ (تكتب بدون ى) لكل الإخوة والأخوات المسلمين والمسلمات ..
أرجو أن تدخل قلوبكم وعقولكم .

لا تنسَ بر والديك و اعطف عليهما واخفض جناحك لهما .. فهو واجب عليك وهو أقل ما يستحقون تجاه تعبهم عليك في صغرك (حتى ولو صدر تقصير منهم) فعظيم حقهم عليك أكبر من حقير حقك عليهم
لا تنسَ سهرهم عليك في مرضك و تعبهم و اجتهادهم لتوفير ما يرضيك و يريحك
لا تنسَ أنك أملهم وحلمهم في تحقيق ما عجزوا عنه .. فلا تكن خيبة أمل لهم
لا تنسَ برهم بعد مماتهم بالدعاء والاستغفار لهم وبر صديقهم
لا تنسَ واجباتك الدينية وأهمها الصلاة والزكاة والصوم وجميع الفرائض
لا تنسَ قدرة الله عليك وعظم عذابه ونقمته كما لا تنسَ سعة رحمته وكريم عفوه
لا تنسَ ذكر الله تعالى في كل وقت وحين والصلاة والسلام على رسوله الكريم محمد صل الله عليه وآله وصحبه وسلم
لا تنسَ عذاب النار لتترك حب الدنيا والمعاصي و لا تنسَ نعيم الجنة لتقبل على الآخرة والطاعات
لا تنسَ أن باب التوبة مفتوح لك إلا إذا حان أجلك أو قامت الساعة .. فبادر إلى التوبة
لا تنسَ الفقير المعدم من الزكاة والصدقة والدعاء والوجه البشوش
لا تنسَ المريض العاجز من العيادة والزيارة والتفاؤل أمامه بالشفاء العاجل ولا تقنطه من رحمة الله .. و لا تنسَ المريض الفقير بالمساعدة بعلاجه
لا تنسَ جارك من السؤال عن حاله ومساعدته والتبسم له
لا تنسَ إبداء النصيحة بالأسلوب الحسن والكلمة الطيبة فتكون ليناً في أمرك بالمعروف ونهيك عن المنكر وتذكر بأن حسن تعاملك قد يهدي المخطئ للصواب وأن غلظتك عليه قد تزيده ضلالاً
لا تنسَ أن كتم العلم فيه إثم كبير .. فلا تبخل على إخوانك بما فتح الله عليك
لا تنسَ الصبر والحلم على من أخطأ بحقك واعتدى عليك
لا تنسَ خفض جناحك و تلطفك مع من هم دونك .. أهلك وعاملك وخادمتك وغيرهم .. وتذكر بأن الراحمون هم من يرحمهم الرحمن وليس قساة القلب الظالمين
لا تنسَ أن طهارة القلب أهم من كثرة العمل الصالح .. فكم من حسنات تكسبها يضيعها فساد القلب بالتكبر على العباد أو الحقد أو الحسد أو الغيبة أو غيرها من أمراض القلوب
لا تنسَ أن الكبرياء لله وحده فقط .. وأنك ضعيف قليل الحلية .. وأن من أعطاك قادر على حرمانك
لا تنسَ إخوانك المجاهدين في كل مكان .. في فلسطين والعراق وأفغانستان وكل مكان
لا تنسَ مساعدتهم ليس فقط بالمال ولكن بالدعاء الصادق المخلص فيه
لا تنسَ أن تحمد الله تعالى وتشكره دائماً على نعمه العظام وأهمها أن أكرمك بالإسلام .. ولا تقدم عليه فخراً أنك من قبيلة أو دولة فكلها إذا لم تكن مسلماً لا تنفعك بشيء يوم الحساب
لا تنسَ أن الدعاء بظهر الغيب لأخيك المسلم يرجع عليك وعليه بالفائدة .. فلا تحرم نفسك منه .

اللهم اغفر للمسلمين والمسلمات والمؤمنين والمؤمنات الأحياء منهم والأموات
اللهم صل وسلم وبارك وأكرم وأنعم على عبدك وحبيبك ورسولك سيدنا محمد النبي الأمي وعلى آله وصحبه والتابعين لهم بإحسان إلى يوم الدين
سبحان ربك رب العزة عما يصفون وسلام على المرسلين والحمد لله رب العالمين